Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 01 June 2005

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

Daily Highlights

- Computer Weekly reports the Bank of America plans to introduce two−factor, two−way authentication to approximately 13 million online banking customers in an attempt to reduce the threat of phishing attacks and identity theft. (See item 4)

- The Associated Press reports a Korean Air flight to California was diverted to Japan after U.S. officials refused to let it enter American airspace because they suspected a passenger might be a terrorist. (See item 8)

- The Associated Press reports that even so−called mild cases of West Nile virus are emerging as bigger health threats than previous thought. (See item 18)

DHS/IAIP Update *Fast Jump*

Production Industries: **Energy**; **Chemical Industry and Hazardous Materials**; **Defense Industrial Base**

Service Industries: **Banking and Finance**; **Transportation and Border Security**; **Postal and Shipping**

Sustenance and Health: **Agriculture**; **Food**; **Water**; **Public Health**

Federal and State: **Government**; **Emergency Services**

IT and Cyber: **Information Technology and Telecommunications**; **Internet Alert Dashboard**

Other: **Commercial Facilities/Real Estate, Monument &Icons**; **General**; **DHS/IAIP Products &Contact Information**

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) – http://esisac.com]

1. *May 29, Associated Press* — **Petroleum may be nearing peak according to experts.** Some observers of the oil industry predict that soon the world's oil production, having grown exuberantly for more than a century, will peak and begin to decline. According to these experts, it will take a decade or more before conservation measures and new technologies can bridge the gap between supply and demand, and even then the situation will be touch and go. However, there are many who doubt the doomsday scenario will ever come true. Most oil industry

analysts think production will continue growing for at least another 30 years. By then, substitute energy sources will be available to ease the transition into a post–petroleum age. "The world has never seen anything like this before and so we just really don't know," said Robert L. Hirsch, an energy analyst at Science Applications International Corp., a Santa Monica, CA, consulting firm. Still, he added, "there's a number of really competent professionals that are very pessimistic." The exact date of the peak doesn't really matter, said Hirsch, because he believes it's already too late. In an analysis he did for the Department of Energy in February, Hirsch concluded that it will take more than a decade for the U.S. economy to adapt to declining oil production.
Source: http://www.washingtonpost.com/wp–dyn/content/article/2005/05/29/AR2005052900083.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *May 28, The Daily Citizen (AK)* — **Arkansas preschool evacuated after chemical blaze.** A chemical fire at Bryce Corporation Plant Two in Searcy, AK caused the evacuation of a Park Avenue preschool that was downwind of emanating gases Friday afternoon, May 27. Searcy Fire Department Captain Lee Reed said the fire never reached inside the plant, but was contained in a distiller machine that separates alcohol–based inks used for printing labels on bags made by Bryce. "In reality it was under control in the sense that they had an automatic sprinkler system," Reed said. "All we did was turn the power off to shut the heater down and then used hose lines to cool the tank, to keep it from over–heating and rupturing." Reed said only carbon monoxide and carbon dioxide came from the distiller, but as a precautionary measure the fire department evacuated 66 students and their teachers from First Step Preschool, which was directly across from the plant, and at the time downwind. The school sent news of their evacuation through the local radio stations announcing that parents could pick the children up at a local church. "We've drilled for such events and it's paid off," Preschool Director Denise Coston said.
Source: http://www.thedailycitizen.com/articles/2005/05/29/news/top_stories/top01.txt

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *May 31, Reuters* — **Israeli police investigate industrial espionage.** Israeli police investigating industrial espionage have detained 18 people, including company executives and private detectives. The probe by the Tel Aviv fraud squad began several months ago and found evidence that Trojan horses, viruses designed to spy on computer systems, had been planted in computers of some of the country's top companies, an Israeli police representative said Sunday,

May 29. The officials the police are investigating work for firms including Israel's top mobile phone operator, Cellcom, and two subsidiaries of dominant phone company Bezeq Israel Telecom –– mobile phone operator Pelephone and satellite television provider Yes. "In this manner of industrial espionage, the private detectives gathered a great deal of information for their clients, who according to suspicions are rival companies," the Tel Aviv police said. A police representative said that two people suspected of creating the Trojan horse, an Israeli who works abroad and his girlfriend, were being held in London and that Israel plans to request their extradition. Among the companies infiltrated by the Trojan horse are the Hot cable television group that competes with Yes, as well as food maker Strauss–Elite, and the Rani Rahav public relations agency, whose clients include Partner Communications, Israel's second biggest mobile phone operator, police said.
Source: http://news.com.com/Israel+police+hold+18+in+industrial+spy+ probe/2100–7348_3–5725976.html?tag=nefd.top

4. *May 31, Computer Weekly* — **Bank of America to use two–factor system to beat phishers.** The Bank of America is to introduce two–factor, two–way authentication to around 13 million online banking customers in an attempt to reduce the threat of phishing attacks and identity theft. Unlike traditional two–factor authentication, the Bank of America's Sitekey approach does not rely on expensive hardware tokens to generate passwords. Instead it uses a customer's PC or handheld device as the second–factor hardware device. Technology from security company Passmark takes a fingerprint of a customer's computer to verify identification. Customers registering for the service choose a picture, write a short phrase and pose three challenge questions to help authenticate the bank to them. When they come to use the service, they enter a login name and see the picture and their phrase, confirming it is the bona fide banking site. The customer then enters a password to use the service. This combined approach is designed to protect against phishing attacks that con users into entering login details into spoof online banking sites, which hackers later use to access their accounts.
Source: http://www.computerweekly.com/Article138764.htm?src=rssNews

5. *May 30, The Times (UK)* — **Sensitive client data may be at risk.** The Tokyo branch of the investment banking giant UBS has launched an internal inquiry into the disappearance of a computer disk thought to contain highly sensitive client information. The loss of the disk is expected to prompt an investigation by the Japanese regulator, the Financial Services Agency (FSA), which was told of the incident on Friday, May 27. According to sources within UBS, the lost disk contains data generated by the bank's equities division and could include confidential trading histories, stop–loss orders and other sensitive information on corporate clients. Internal safeguards would normally be expected to prevent sensitive information from being stored on portable disks of the sort that is now missing. In a number of financial institutions client data is often saved on network servers that never leave the building. A new law requiring Japanese companies to improve data protection came into force in April.
Source: http://business.timesonline.co.uk/article/0,,8209–1633534,00_.html

6. *May 29, Boca Raton News (FL)* — **U.S. military tries to solve identity theft with cyber technology.** The U.S. military is seeking the ultimate answer to identity theft and Internet hacking in a physics–based cyber security system developed five years ago in a private Boca Raton, FL, laboratory. A team of top war games scientists from the U.S. Joint Forces Command's Joint Futures Laboratory (JFL) and other military agencies attempted to hack 100

prototype units of the Location Specific Digital Fingerprint (LSDF) system invented in at Digital Authentication Technologies Inc. Traditional computer encryption systems, currently used by most government data brokers and large financial companies, fight hackers by using mathematical formulas to generate semi−random numbers for an electronic security code. However, such systems are vulnerable to skilled hackers who can puzzle out the mathematical formulas from a remote location or simply steal the login password. By contrast, the new LSDF system encrypts computers by generating its encryption numbers from a measurement of the physical environment around the workstation, instead of from a deducible formula. Since the random encryptions are based on the particular physical environment around the computer, the system cannot be spoofed by a hacker from a remote location.
U.S. Joint Forces Command's Joint Futures Laboratory:
http://www.jfcom.mil/about/fact_jfl.htm
Source: http://www.bocanews.com/index.php?src=news&category=Local%20 News&prid=11724

7. *May 28, Associated Press* — **State officials warning Medi−Cal recipients about identity theft possibility.** California health officials have begun notifying more than 20,000 Medi−Cal recipients that they could become targets of identity theft because a laptop computer was stolen. The computer, which contained the names, Social Security numbers and health information about 21,600 Medi−Cal recipients, was stolen from the trunk of a car belonging to an employee of a company that provides the state with data services. Ken August, a spokesperson for the California Department of Health Services, said that the laptop was not encrypted. Medi−Cal provides health care for low−income Californians.
Source: http://www.sanluisobispo.com/mld/sanluisobispo/11764302.htm

[Return to top]

Transportation and Border Security Sector

8. *May 31, Associated Press* — **Korean Air flight to San Francisco diverted to Japan.** A Korean Air flight to California was diverted to Japan after U.S. officials refused to let it enter American airspace because they suspected a passenger might be a terrorist, airline officials said Tuesday, May 31. The man, a U.S. citizen of Pakistani descent, has the same name as that of a suspect on the U.S. government's no−fly list. He was allowed to reboard the flight with other passengers when it was determined he was not the suspect in question, and the flight continued to San Francisco. The man and his family had boarded a connecting flight in Bangkok before arriving in South Korea for the flight to San Francisco.
Source: http://www.usatoday.com/news/world/2005−05−31−koreanair−flig ht_x.htm

9. *May 31, Associated Press* — **Plane crashes at Teterboro Airport.** A small plane crashed Tuesday morning, May 31, at New Jersey's Teterboro Airport, a busy center for business and private planes outside New York City, injuring one of the two people on board, authorities said. The Swearingen turboprop was on final approach to the airport when the pilot reported engine problems, the Federal Aviation Administration said. It was the third accident this year at Teterboro Airport, about 12 miles west of midtown Manhattan. Teterboro has grown into one of the nation's busiest small airports, catering to corporate jets. It had 202,720 arrivals and departures in 2004, a four percent increase from 2003, officials said.

10. *May 31, Associated Press* — **United Airlines' mechanics ratify deal.** United Airlines' mechanics union ratified a five−year contract Tuesday, May 31, removing one strike threat from the carrier as another labor group negotiated down to the deadline. A majority of the 7,000 members of the Aircraft Mechanics Fraternal Association voted to accept a five−year pact entailing $96 million in annual reductions and 3.9 percent pay cuts, among other conditions. The company released a statement saying it appreciated the approval vote. "This is an important and necessary step in providing the cost savings United needs to finish its restructuring successfully," the airline said. The new pay cuts, effective immediately, will come on top of 14 percent reductions made two years ago. Reduced benefits, such as sick days and holidays, would account for the rest of the labor savings. A five percent defined−contribution pension plan is part of the new contract, replacing the former defined−benefits plan. The mechanics' union also will get $40 million in convertible notes upon United's exit from Chapter 11 bankruptcy.
Source: http://news.yahoo.com/s/ap/20050531/ap_on_bi_ge/united_airli nes

11. *May 31, Kansas City Star (MO)* — **Retirement coming soon for traffic controllers.** Nearly three−quarters of the nation's nearly 15,000 air traffic controllers will reach retirement age within the next nine years. The vast bulk of those come from the wave of new hires made after President Reagan fired more than 10,000 striking air traffic controllers in 1981. To deal with the impending retirements, the Federal Aviation Administration (FAA) hopes to hire 12,500 new air traffic controllers in the coming years. President Bush's 2006 budget included money to hire 595 new controllers, on top of the FAA's plan to hire replacements for all 654 controllers set to retire this year. Aviation observers say the continued safety and efficiency of air travel is at stake. FAA spokesperson Tony Molinaro said: "We do have the plan in place and we feel we have the time to make it work and get people in place, fully trained." To help the process along, the FAA hopes to train new controllers more quickly and to get more productivity out of new recruits. But some question the FAA's efforts, wondering if the hiring is fast enough and whether the agency might better spend money on a more dramatic overhaul of the way airplanes fly.
Source: http://www.kansascity.com/mld/kansascity/business/11775989.h tm

12. *May 27, Department of Transportation* — **Infrastructure improvement grant for Alaska Railroad.** The Federal Railroad Administration (FRA) announced on Friday, May 27, a $24.8 million infrastructure grant for the Alaska Railroad to upgrade mainline tracks, replace bridges, prevent rock slides and install track at the new Fairbanks Intermodal Facility. The Alaska Railroad is a state−owned corporation providing both passenger and freight rail services to communities from Fairbanks to Seward. Additionally, through innovative arrangements with cruise line companies, the railroad has developed a special service tailored to meet the needs of the cruise industry. By attaching first−class travel cars owned by the cruise lines to its trains, the railroad brings cruise passengers to places in Alaska that ships cannot serve. This innovative service has helped make the railroad unique as the only profitable passenger railroad in the nation, receiving no state operating subsidy. The grant involves replacement of nearly 16,000 railroad ties and conversion of 30 miles of track, from jointed to continuously welded rail, for easier maintenance and a smoother ride. These funds also will be used to stabilize track

subgrades, prevent rock slides onto tracks near Healy Canyon, and build additional track at the Fairbanks Intermodal Facility to handle more trains, more efficiently. Also, nine bridges will either be replaced or rehabilitated.
Source: http://www.dot.gov/affairs/fra1005.htm

13. *April 29, Government Accountability Office* — **GAO–05–266: Federal Aviation Administration: Stronger Architecture Program Needed to Guide Systems Modernization Efforts (Report).** The Federal Aviation Administration's (FAA) mission is to promote the safe, orderly, and expeditious flow of air traffic in the U.S. airspace system. To this end, FAA is modernizing its air traffic control systems, a multibillion dollar effort that the Government Accountability Office (GAO) has designated as a high–risk program. GAO's research into the practices of successful public– and private– sector organizations has shown that developing and using an enterprise architecture, or blueprint, to guide and constrain systems investments is crucial to the success of such a modernization effort. GAO was asked to determine whether FAA has established effective processes for managing the development and implementation of an enterprise architecture. To support the agency in its efforts to develop and implement an enterprise architecture, GAO is making recommendations to the Secretary of Transportation for establishing an effective enterprise architecture management program, beginning with demonstrating senior management commitment and support for the program. The Department of Transportation provided technical comments on a draft of this report. GAO has incorporated these, as appropriate, in the report.
Highlights: http://www.gao.gov/highlights/d05266high.pdf
Source: http://www.gao.gov/cgi–bin/getrpt?GAO–05–266

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

14. *May 31, RFID Journal* — **New York tests radio frequency identification on domestic deer.** New York's Department of Agriculture and Markets will begin this month a pilot program testing UHF RFID (radio frequency identification) tags on the state's domestic deer and elk. The ultimate goal is to track the cervid population and better trace diseases. The program will use a 915 MHz radio frequency identification system that allows deer and elk tags to be read from as far away as eight feet. New York requires that all cervid farmers inventory their herds annually, which can be done by means of a simple head count at small farms, or by visual numeric tags or bar codes. With this pilot, the Department of Agriculture and Markets hopes to determine if cervid farmers can use the RFID system to easily take annual inventory of their herds and trace where the animals have been. If a diseased animal is found, it might then be possible to trace it back to other farms where it had been and any other cervids it had come in contact with. To accomplish this, farmers would need to use RFID tags and readers, as well as have access to a statewide software system. The current pilot, however, is intended to address

only hardware issues.
Source: http://www.rfidjournal.com/article/articleview/1623/1/1/

15. *May 30, Associated Press* — **Federal officials prepare for possible loss of Great Lakes ash tree stock.** Federal officials are preparing should the emerald ash borer kill off the Great Lakes region's entire ash tree stock by collecting and safekeeping seeds to reintroduce the tree years from now. The seed collection program began earlier this year with the federal Natural Resources Conservation Service, a division of the U.S. Department of Agriculture. The service's Rose Lake Plant Materials Center in East Lansing, MI, is undertaking the project. Center manager John Leif said the program asks state residents to identify ash trees near them. When ash tree seeds darken and begin to fall to the ground, people are asked to send them to the center, Leif said. There they will be inventoried and sent on to the National Center for Genetic Resources Preservation in Fort Collins, CO, he said. Saved ash seeds could be used in the future through cloning, direct planting, or in some other way to begin restoring the Great Lakes region's ash population. The emerald ash borer was discovered in southeast Michigan in July 2002. State officials believe the beetle came to Michigan from Southeast Asia in packing materials. An estimated 15 million of the state's 700 million ash trees are already dead or dying from ash borer larval infestations in southeastern Michigan counties.
Source: http://www.freep.com/news/statewire/sw116496_20050530.htm

[Return to top]

Food Sector

16. *May 30, Food Safety and Inspection Service* — **Ready−to−eat meat products recalled.** Winter Sausage Manufacturing, an East Pointe, MI, firm is recalling approximately 363,332 pounds of ready−to−eat meat products that may be contaminated with Listeria Monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Monday, May 30. The problem was discovered through routine FSIS testing. FSIS has received no reports of illnesses associated with consumption of these products. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/PDF/Recall_025_2005_Release.pdf

17. *May 27, Food and Drug Administration* — **Tomatoes recalled.** California Specialty Produce, Inc. of Vista, CA, is recalling Red Pear Tomatoes, because they have the potential of being contaminated with Salmonella, an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. Healthy persons infected with Salmonella often experience fever, diarrhea, nausea, vomiting, and abdominal pain. In rare circumstances, infection with Salmonella can result in the organism getting into the bloodstream and producing more severe illnesses such as arterial infections, endocarditis, and arthritis. Red Pear Tomatoes were shipped to wholesalers who are restaurant suppliers in New York, California, and Colorado. No illnesses have been reported to date. The recall was as the result of a routine sampling program by the Food and Drug Administration, which revealed that the products contained the bacteria.
Source: http://www.fda.gov/oc/po/firmrecalls/caspecialty05_05.html

Water Sector

Nothing to report.

Public Health Sector

18. *May 31, Associated Press* –– **Mild cases of West Nile emerge as bigger threat.** West Nile has long been considered a serious problem for the elderly and frail, and more of a nuisance illness for everyone else. Now a surprising number of patients show the virus is more threatening than widely believed –– even so–called mild cases of West Nile fever can impair people for months. "West Nile is fading a little bit from the public consciousness," worries Henry Masur of the National Institutes of Health. "Still, there are more cases of paralysis than there were in many years of polio." West Nile appeared in New York City in 1999 and began an inexorable march across the U.S. Since then, the U.S. Centers for Disease Control and Prevention (CDC) has counted more than 16,600 human cases and 654 deaths. Severe illness still is rare, considering that 80 percent of people infected never show symptoms. But last year, about a third of the West Nile cases reported to the CDC had neurologic complications. They are most common in older adults. Then there are patients who came down with West Nile's most perplexing complication: polio–like paralysis or severe muscle weakness that can strike healthy people in their 30s, 40s, and 50s.
Source: http://www.lsj.com/apps/pbcs.dll/article?AID=/20050531/LIFE02/505310326/1079/life

19. *May 31, Associated Press* –– **Polio cases rise in Yemen.** The number of confirmed cases of polio in Yemen has reached 179, including 71 new cases in less than a week, the World Health Organization (WHO) said Tuesday, May 31. David Heyman, the WHO's polio chief, said an immunization drive in Yemen –– which until April was believed to be polio–free –– should be able to "break the back of polio" with a new, more effective vaccine. Older vaccines were designed to combat each of the three types of polio in existence but were less effective against the Type I virus present in Yemen, Heyman said. The new "monovalic" vaccine is designed specifically for Type I polio and can immunize up to 20 percent more children after a single dose and up to 100 percent after repeated vaccination, he said. There have been no new cases of Type II since it was successfully eradicated in 1999 and Type III has become increasingly rare, he said. Yemen is one of 16 previously polio–free countries that has reported new cases since 2003 after a vaccine boycott in Nigeria was blamed for causing an outbreak that spread the disease to other countries.
Source: http://news.yahoo.com/s/ap/20050531/ap_on_he_me/un_yemen_polio;_ylt=Ajpbi497KC8PCqWCDhDpbDVZ24cA;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

20. *May 31, Associated Press* –– **Inverness to buy Abbott Labs tests.** Inverness Medical Innovations Inc., a maker of medical tests and vitamin supplements, said Tuesday, May 31, that

it is buying certain disease tests from Abbott Laboratories for $56.5 million. Abbott's Determine and DainaScreen diagnostic tests quickly detect diseases such as hepatitis and syphilis, as well as HIV, the virus that causes AIDS, Inverness said. Under the agreement, Inverness will acquire manufacturing equipment along with ownership of or licenses for intellectual property related to the products. Determine and DataStream posted sales of about $23 million in 2004, Inverness said. The two products are currently part of Abbott's rapid diagnostics business. Abbott will continue to distribute the Determine−brand products, which are sold outside of the U.S., for about two and a half years.
Source: http://www.businessweek.com/ap/financialnews/D8AE8JP80.htm?campaign_id=apn_home_down

21. *May 27, Reuters* — **Emergency room visits on the rise in U.S.** Crowding in U.S. emergency departments is being fueled by rising numbers of patients even as some departments shut their doors. Catharine W. Burt and Linda F. McCraig, at the U.S. Centers for Disease Control and Prevention's Division of Health Care Statistics, report the annual number of emergency department (ED) visits increased from 90.3 million to 113.9 million visits between 1993 and 2003. However, the number of hospital EDs in the U.S. decreased by about 14 percent during the same period. Fifteen percent of visits were classified as emergencies (requiring treatment in less than 15 minutes) and 35 percent were urgent (treatment required within one hour). Thirteen percent were non−urgent. The greatest increase in rates was among adults. For those age 65 and older, ED visit rates increased by 26 percent over the last decade. "As America's elderly population continues to grow, we expect to see even more elderly patients in the coming years," Robert Suter, president of the American College of Emergency Physicians noted.
Source: http://news.yahoo.com/s/nm/20050527/hl_nm/er_increase_dc;_ylt=Ak_FVCnVkUevwSt1i.inzIMQ.3QA;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

22. *May 31, Federal Computer Week* — **Virginia Tech studies battlefield wireless.** Virginia Polytechnic Institute and State University won a $246,000 Department of Defense (DoD) grant to create a test bed platform that will probe ways to integrate various battlefield wireless networks, research that could also help overcome interoperability problems that plague emergency workers and first responders. DoD wants to develop a network−centric communications infrastructure, said Thomas Hou, an assistant professor of electrical engineering at Virginia Tech and principal investigator on the project, but certain kinds of wireless networks can't yet talk to each other. Mobile ad hoc networks are ideal for keeping military groups on the move connected to one another, while stationary wireless−sensor networks relay valuable observational data from areas that are hostile to humans. Having the

two kinds of networks interoperate would have obvious advantages. The results of these studies should also be applicable to network applications used for homeland security, law enforcement and anti−terrorism, he said.
Source: http://www.fcw.com/article89023−05−31−05−Web

23. *May 31, Bossier Press−Tribune (LA)* — **Citizens receive response training.** In the event of a large−scale emergency or disaster, local authorities are not the only ones prepared to hit the streets to lend a helping hand. Following a hands−on training session Saturday morning, May 28, 14 members of the Bossier−Shreveport, LA, community joined the Community Emergency Response Team (CERT) and are prepared to utilize their new sills to help save lives. The training Saturday morning was the culmination of 20 hours of training the volunteers underwent over the past four weeks. The scenarios included a Hazmat situation involving a burning building, an automobile crash and several incidents involving fallen power lines. The CERT program was established in the local area in 2003, and falls under the programs of the FreedomCorps, which was established shortly after September 11, 2001. Four times a year the Caddo−Bossier Office of Homeland Security and Emergency Preparedness holds training sessions for citizens wishing to become part of a volunteer group armed with emergency response skills such as emergency medical operations, search and rescue, disaster psychology and terrorism awareness, among other things. While they are not being trained to be first responders, these volunteers are equipped with the knowledge to assist emergency teams or keep a situation under control until responders arrive.
Source: http://www.bossierpress.com/index.php?option=com_content&task=view&id=833&Itemid=2

24. *May 31, NBC 17 (NC)* — **Study: Nursing homes could be safe havens in disasters.** A nursing home may not seem like the safest harbor in a storm, but a researcher at RTI International says it might actually be an excellent place to provide shelter, storage and emergency medical treatment in a disaster. Lucy A. Savitz is a health services researcher at North Carolina's Research Triangle Institute (RTI), the nonprofit scientific research and technology development corporation. In a study she recently completed for the federal Agency for Healthcare Research and Quality, Savitz found that nursing homes have the potential to contribute to their larger communities in times of public−health emergency. They can serve as alternative treatment centers, provide shelter to the displaced, and store hazardous material gear and other supplies, she said. Involving the homes in planning would be good for their own sake, Savitz found. Her research also examined the homes' own emergency response plans and what special needs they might have if threatening situations arise. She found that most nursing homes have plans for natural disasters, but not for such man−made catastrophes as bioterrorism responses. Savitz said many nursing homes rely on the American Red Cross for disaster relief, but that could overwhelm the nonprofit organization.
Source: http://www.nbc17.com/news/4548349/detail.html

[Return to top]

Information Technology and Telecommunications Sector

25. *June 01, FrSIRT* — **PeerCast malformed URL remote format string vulnerability.** A vulnerability was identified in PeerCast, which may be exploited by remote attackers to execute

arbitrary commands or cause a denial of service. This flaw is due to a format string error when handling specially crafted HTTP requests (port 7144), which may be exploited by remote attackers to crash or compromise a vulnerable server. Upgrade to PeerCast version 0.1212: http://www.peercast.org/download.php
Source: http://www.frsirt.com/english/advisories/2005/0651

26. *May 30, SecurityFocus* — **Microsoft Windows Remote Desktop protocol server private key disclosure vulnerability.** The vulnerability presents itself because a private key that is used to sign the Terminal Server public key is hardcoded in a DLL. This allows the attacker to disclose the key and calculate a valid signature to carry out man in the middle attacks. An attacker could therefore cause the client to connect to a server under their control and send the client a public key to which they possess the private key. There is no solution at this time.
Source: http://www.securityfocus.com/bid/13818/info/

<div align="center">

Internet Alert Dashboard

</div>

<div align="center">

DHS/US−CERT Watch Synopsis

</div>

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports a remote exploitation of a format string vulnerability in the imap4d server within version 0.6 of the GNU Project's Mailutils package could allow an unauthenticated attacker to execute arbitrary code. The imap4d server allows remote users to retrieve their email via the Internet Message Access Protocol, Version 4rev1 as specified in RFC3501. This is a client/server protocol supported by a large number of email clients on multiple platforms.

<div align="center">

Current Port Attacks

</div>

Top 10 Target Ports	135 (epmap), 445 (microsoft−ds), 1026 (−−−), 1027 (icq), 1433 (ms−sql−s), 1434 (ms−sql−m), 4899 (radmin), 139 (netbios−ssn), 1028 (−−−), 25 (smtp)

Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

27. *May 31, Government Accountability Office* — **GAO−05−547: Olympic Security: U.S. Support to Athens Games Provides Lessons for Future Olympics (Report).** The 2004 Summer Olympics in Athens, Greece, were held against the backdrop of growing concerns about international terrorism. Despite widespread fears of a potential terrorist attack on the Olympics, Greece hosted a safe and secure event with no terrorist incidents. To assist Greece in securing the 2004 Games, U.S. government agencies provided training and other support in the four years leading up to the Games. In addition, the U.S. government provided some security and other assistance to American athletes, spectators, and commercial investors, and expects to continue such support for future Olympics, including the upcoming 2006 Winter Olympics in Turin, Italy. The Government Accountability Office was asked to (1) determine the U.S. approach and coordination efforts for providing security assistance to the 2004 Summer Olympics; (2) examine the roles of U.S. agencies in Athens Olympics security and their financial outlays; and (3) review lessons learned in providing security assistance in support of the Olympics and how they are being incorporated into preparations for future Olympics. The Departments of State, Homeland Security, Defense, and Justice concurred with the report or had no comments.
Highlights: http://www.gao.gov/highlights/d05547high.pdf
Source: http://www.gao.gov/new.items/d05547.pdf

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins – DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us–cert.gov or visit their Web page at www.us–cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.